CS 70 Discrete Mathematics and Probability Theory
Summer 2026 Tate

HW 02

Due: Saturday, 7/11, 4:00 PM
Grace period until Saturday, 7/11, 6:00 PM
Remember to show your work for all problems!

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Celebrate and Remember Textiles

Note 6

You've decided to knit a 70-themed baby blanket as a gift for your cousin and want to incorporate rows from three different stitch patterns with the following requirements on the row lengths:

- Alternating Link: Multiple of 8, plus 3
- Double Helix: Multiple of 3, plus 1
- Crossover: Multiple of 7, plus 6

You want to be able to switch between knitting these different patterns without changing the number of stitches on the needle, so you must use a number of stitches that simultaneously meets the requirements of all three patterns.

Find the *smallest number of stitches* you need to cast on in order to incorporate all three patterns in your baby blanket.

2 RSA Practice

Note 7

Consider the following RSA scheme: we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$.

(a) What is the decryption key d? Calculate its exact value.

(b) If the receiver receives 4, what was the original message?

(c) Encrypt your answer from part (b) to check its correctness.

3 Tweaking RSA

Note 7

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original RSA system, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

(a) Show how you choose $e, d > 1$ in the encryption and decryption function, respectively. Prove the correctness property: the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve now compute d in the decryption function? If so, by what algorithm?

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain the modifications made to encryption and decryption and include a proof of correctness showing that $D(E(x)) = x$.

4 Equivalent Polynomials

Note 7
Note 8

This problem is about polynomials with coefficients in GF(p) for some prime $p \in \mathbb{N}$. We say that two such polynomials f and g are *equivalent* if $f(x) \equiv g(x) \pmod{p}$ for every $x \in \text{GF}(p)$.

(a) Show that $f(x) = x^{p-1}$ and $g(x) = 1$ are **not** equivalent polynomials under GF(p).

(b) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 13 that is equivalent to $f(x) = x^{13}$ over GF(13); then find a polynomial with degree strictly less than 7 that is equivalent to $g(x) = 4x^{78} + 6x^7 + 3$ over GF(7).

(c) In GF(p), prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

5 Cal Football's Secrets

Note 8

After a tough defeat, the Cal Football team has created a new set of top-secret plays. They're worried about leaks, however, and have asked you to devise a secret sharing scheme to protect their strategy.

The team has one head coach, six assistant coaches, and thirty-two players. All the top-secret plays are encrypted with a secret code and we know that:

- The head coach along with one assistant coach should be able to access the plays.
- The majority (4+) of assistant coaches should be able to access the plays.
- All thirty-two players together should be able to access the plays.
- Sixteen players and two assistant coaches should be able to access the plays.

Design a secret sharing scheme to make this work.

6 Extra Points in Lagrange Interpolation

Note 8
Note 9

A spaceship's safe is locked with a secret code s. The security system stores the secret using a **degree-2** polynomial $P(x)$ over GF(7), where $P(-1) = P(6) = s$. Crew members Alice, Bob, Eve, Mallory, and Trent are each given a point on $P(x)$ so that they can work together to unlock the safe:

Crew Member	Alice	Bob	Eve	Mallory	Trent
Point	(0, 1)	(1, 3)	(2, 0)	(3, 0)	(4, 0)

(a) The crew members gather to unlock the safe using Lagrange interpolation. Bob starts by computing his Lagrange basis polynomial using all 5 points:

$$\Delta_{\text{Bob}}(x) = x^4 + 5x^3 + 5x^2 + 4x \pmod 7$$

Help the crew finish the interpolation to find the recovered polynomial $P'(x)$ and secret code.

[*Hint*: Look closely at the points before doing Lagrange interpolation.]

(b) The secret code obtained in part (a) is wrong, and the crew suspects that exactly one of the points is incorrect; they will try to fix it using Berlekamp-Welch. Set up, but do not solve, a system of linear equations the crew will use to identify the incorrect point.

(c) The crew figure out that Mallory's point $(3,0)$ is incorrect. Knowing this new information, help the crew recover the correct $P(x)$ and true secret code s.

7 Error-Correcting Codes

Note 9

(a) Recall from class the error-correcting code for erasure errors, which protects against up to k lost packets by sending a total of $n+k$ packets (where n is the number of packets in the original message). Often the number of packets lost is not some fixed number k, but rather a *fraction* of the number of packets sent.

Suppose we wish to protect against a fraction α of lost packets (where $0 < \alpha < 1$). At least how many packets do we need to send (as a function of n and α)?

[*Hint*: the answer is not $n + \alpha n$.]

(b) Repeat part (a) for the case of general errors.

8 (Optional) Anonymous Feedback Form

Please fill out this optional form to let us know how you are doing in CS 70 and how you are absorbing the course material: https://forms.gle/A8eqVTXKg4nJ5VM8A!